Systematic Literature Review (SLR) of Resource Scheduling and Security in Cloud Computing

Abdullah Sheikh[1], Malcolm Munro[2], David Budgen[3]
Department of Computer Science, Durham University
Durham, United Kingdom

***Abstract*—Resource scheduling in cloud computing is a complex task due to the number and variety of resources available and the volatility of usage-patterns of resources considering that the resource setting is on the service provider. This compounded further when security issues are also factored in. This paper provide a Systematic Literature Review (SLR) that will help to identify as much prior relevant research that has been done in the area of research topic. Also, all papers that are found from the search will be classified into groups to stand on the current situation and to identify possible existing gaps.**

***Keywords*—Cloud computing; security; resource scheduling; systematic literature review; SLR**

I. Introduction

Scheduling in cloud computing is a process or mechanism applied 'to minimise wasting limited resources by efficiently allocating them among all active nodes' [1]. Nodes or virtual machines (VMs) are the virtual resources that are assigned to consumers for running the service and executing tasks [2]. Scheduling is a very complex operation in cloud computing used to allocate resources, improving server utilisation, enhance service performance, and executing tasks [3].

Scheduling can use either static or dynamic methods for scheduling resources in cloud computing. These methods can provide sufficient use of cloud resources to meet Quality of Service (QoS) requirements [4]. Furthermore, using scheduling techniques can avoid conflicts in allocating active resources. For example, scheduling can avoid duplication of allocating the same virtual resource at one time. Also, it can help manage limited resources by handling high demand of requests by using dynamic method that can update the system regularly and to execute tasks over resources based on the resources availability. However, there are some issues need to be considered such as security, limited resources, virtual machines and applications.

Executing and running tasks over the allocated resources raises some security issues that need to be considered such as data security, and service security. Data security includes privacy, integrity, protection from any threats and attacks. Service security includes resource security, and privacy. So, there is a need to consider these issues and the security constraints, including data security, and availability to get an optimised resource scheduling. For this research, the main focus will be on resource scheduling mechanisms when security is factored into the cloud model.

According to Singh and Chana, [5], there are two main objectives for resource scheduling as follows:

1) Workloads refer to the tasks that consumers want to run over the resources. So, identifying suitable resources for scheduling workloads on time will help to enhance the effectiveness of resource utilisation.
2) To identify heterogeneous multiple workloads to fulfil the Quality of Service (QoS) requirements, such as CPU utilisation, availability, reliability and security.

This paper focuses on searching and reviewing prior research relevant to resource scheduling and security in cloud computing and to identify possible existing gaps.

This paper is organised as follows. Section II gives an over view of cloud computing including cloud definition, cloud architecture, obstacles facing cloud growth, research method, explaining why SLR is important to this research, and research questions and research scope. Section III discusses the search strategy including identifying the search period, search strings, search engines. Section IV describes the inclusion/exclusion criteria, and the procedures of selection. Section V explains the aim of SLR. Section VI presents how the data will be extracted from each paper. Section VII discusses the synthesis strategy and the threats of validity. Section VIII explains limitation and factors that could affect this research. Section IX presents discussion of current finding and proposed solution. Section X concludes with suggestion and future work.

II. Background

This section serves as a background and a general view of cloud computing, basic cloud architecture and cloud features. Also, it shows the considered top ten obstacles that are facing the growth of cloud computing and how they related to the security in the cloud. Then it presents the research method for this Systematic Literature Review (SLR). After that, it explains why this SLR need to be performed followed by research questions and the research scope.

A. Cloud Definition

There are many different definitions of cloud computing, the National Institute of Standard and Technology (NIST) [6] gives a basic definition of cloud computing as "a model for enabling convenient, on-demand network access to a shared pool configurable computing resources (e.g. networks, servers, storage, application, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

To obtain a cloud service a consumer needs to contact a service provider. This communication process makes the

consumer and the provider reach an agreement of the level of the service. This agreement referred to Service Level Agreement (SLA) [7]. This SLA is the basis for the expected level of the service between the consumer and the provider. The provider of a cloud architecture can offer various services to a consumer. Quality of Service (QoS) refers to cloud stakeholders expectation of obtaining a desirable service meeting requirements such as timeliness, scalability, high availability, trust and security specified in the Service Level of Agreement SLA [8]. For this research, Quality of Service (QoS) includes the following concerns:

- Security: Security is a shared responsibility between cloud providers and consumers to ensure that the level of security is at a desired level. Consumers need to be aware of security from their side and protect their service from any threats. Cloud providers are able to achieve better scalability by running multiple virtual machines on physical machines. They have to defend the service against any security risks from any unauthorised physical access, data security, security software, and resource security. Other cloud providers who do not use virtual machine have to secure servers and data storage from any security risks. Then any security risks in the virtualisation technology that allows co-occupant virtual machines to make unauthorised access could compromise information assets of consumers [9].
- Service Performance: A consumer requires a certain level of the service performance will need provider guarantees to run the require service in the cloud. The Service Level Agreement (SLA) is an agreement between a service provider and a consumer, that specify the level of the service provided [8] [9] [10]. Also, both provider and consumer follow the rules and conditions of this agreement to keep the service secure without any security issues.

These services can vary both in terms of functionality (such as storage capacity or processor count) or in terms of the Quality of Service (QoS) provided [11]. In terms of the QoS a provider will offer a defined SLA which the consumer can use when determining the 'best' provider for their needs.

According to Mell and Grance [6], the cloud architecture is a combination of the following three components:

- **Essential Characteristics:** The essential characteristics refer to a set of cloud features that allow providers and consumers managing, accessing, and measuring the cloud services and resources. These characteristics provide cloud providers and consumers different level of control to measure and provision the service. From a security prospective, each characteristic has a different security concern for both provider and consumers. These security concerns include access control and data security [2]. Access control includes accessing, managing the service, and access availability. Data security includes data confidentiality, date integrity, and data availability.
  The five essential cloud characteristics are:
  1) On-demand self-service: A consumer can manage and control the service resources such as sever time and network storage without any physical interactions by the provider.
  2) Broad network access: Consumers can access and use the cloud service from anywhere across the network.
  3) Resource pooling: Providers can serve consumers with different resources according to consumer demand. Resources such as storage, processing, physical machine, and network bandwidth [2]. Consumers do not need to be concerned about physical location of resources.
  4) Rapid elasticity: Resources can be rapidly scaled outward or inward at any time according to consumers demand.
  5) Measured service: Measured service is the ability to track and control the usage of the resources which can be performed by consumers.
- **Service Models:** Service models in the cloud defines to a consumer the type of the system management and system operations and type of the access to cloud systems. According to Nallur et al. [9] service availability, security and performance are the main elements that are considered to affect cloud service in the service models. Based on SLA, consumers have to trust the provider on the service availability and the only concern is if there is any downtime to the service it will be the time of the service recovery to obtain the service again. The recovery process is the responsibility of the service provider based on the SLA. Both provider and consumers are involve in security such as data security and protection. The provider is concerned about providing a secure and reliable service via the network. Service performance means that the service provided to consumers at a satisfactory level and good quality. There are three types of service model, each service model provides different capabilities to obtain the service:
  1) Infrastructure as a Service (IaaS): To provide a basic form of the service such as a virtual machine (VM), virtual storage and network bandwidth [9]. Consumers have to configure the setting and install any needed operating system and software before running the service. One of the main security concerns in IaaS for the provider is to check that there is no VMs interference while the service is running.
  2) Software as a Service (SaaS): Here, software and applications are provided by the cloud provider which lets consumers use these applications. Consumers can have access to the service from different devices via different interface such as web browser and a program interface. One security concern needs to be considered is web browser security. The level of the browser security is very important, weak browser security can let an attacker get important information or hijack the consumer resources and data.

3) Platform as a Service (PaaS): In this form, the cloud provider provides a platform that allows the consumer to develop their application but the cloud provider is still responsible for maintenance and all upgrades of the platform.

Table I shows the main security issues that exists for each service model [12]. From Table I, SaaS has the most security issues because it is more complex than the other service models. PaaS and IaaS have less security issues compared with SaaS because they have better control over the security and they are not involved in the application level.

Table I shows the responsibility perspective for the the security issues for providers and consumers. These issues are different in terms of responsibilities from the providers and consumers. The table shows that most responsibility to ensure the security level of the service is on the providers. The providers responsibilities include data (security, locality, segregation, confidentiality), network security, authentication and authorisation, vulnerability in virtualisation, availability, and identity management. Using secure web applications to access the service is mostly the responsibility of the consumers. The other security issues such as data access, data breaches and backup are shared responsibilities for providers and consumers. These security issues affect differently each service model. These issues are:

- Data Security: Providers need to use good techniques to secure data access such as encryption and decryption.
- Network Security: To secure the data flow through the network from any security breach or leakage.
- Data Locality: To manage storing consumers data in a reliable location and to protect it from any risks.
- Data Integrity: To make sure that data is stored and then it correctly and accurately flow through the database over the service.
- Data Segregation: To secure the data flow, and data storage from any intrusions hacking the system on each level of the service.
- Data Access: To control data access for consumers.
- Authorisation, Authentication: To manage accessing to the service or database.
- Data Confidentiality: To control and protect the data flow on each level of the service.
- Web Application Security: Consumers need to ensure their web applications are secure to access to the service.
- Data Breaches: Providers need to protect data and prevent any indirect access.
- Vulnerability in Virtualisation: Providers need to ensure that each tasks executed separately from each other to reduce security risks that could occur.
- Availability: Providers need to ensure that the service is delivered on demand.
- Backup: The backup information is important and if it has been hacked then any unauthorised accessed will cause a security issues for the consumers. Providers need to ensure that backup is taken regularly and be secured and encrypted to make the service more reliable and fast recovery when it required.
- Identity Management: To control and check the identity of accessing to the service and resources by identifying all information that used to log in.

TABLE I. SECURITY ISSUES IN THE SERVICE MODELS [12]

Security Issues	Service Models			Responsibility Prospective	
	IaaS	PaaS	SaaS	Providers	Consumers
Data Security	√	√	√	√	
Network Security	√	√	√	√	
Data Locality	√		√	√	
Data Integrity		√	√	√	
Data Segregation			√	√	
Data Access	√	√	√	√	√
Authorisation, Authentication	√		√	√	
Data Confidentiality			√	√	
Web Application Security			√		√
Data Breaches	√		√		√
Vulnerability in Virtualisation	√	√	√	√	
Availability	√	√	√	√	
Backup			√	√	√
Identity Management	√		√	√	

Subashini and Kavitha [12] claim that the security issues in the service models such as data security and network security make a significant trade-off to each service model to obtain a reliable, trusted and secure services.

These service models offer different features to customers and providers to operate the service. SaaS offers many significant benefits to customers such as service efficiency improvement and reduced costs. In SaaS providers do all provisioning for hardware, data storage, power, virtual resources. As a result consumers have to pay for what they use, and there is no upfront cost for anything else. With all the benefits that are provided in SaaS, it has some issues such as lack of visibility of data stored and security.

In PaaS users can build their application on top of the platform, but this feature raises the security risks for all the services. Building applications on top of the platform increase security risks such as data security and network intrusion by unlocking the way to intruders trying any unauthorised actions [12]. For example, hackers can attack the applications code and run a very large amount of malicious programs to attack the service. In IaaS, consumers can get services with less cost with basic security configuration and less load balance. Providers have to ensure that the service infrastructure is highly secure for, data storage, data security, data transmission, and network security.

- **Deployment Models:** Deployment models are to describe how the cloud services deliver to consumers. According to [13] there are many security concerns on the cloud deployment models including data privacy and trust, policies, and data transfer. As a result of these concerns providers have to secure cloud services. Also, providers need to apply security policies that can

handle data access and security. The four deployment models, which specify the availability of using cloud service [6], are:

1) Public: To specify that cloud services is accessible with no restriction for all users.
2) Private: To make cloud services available to particular single group.
3) Community: To make cloud services shared between limited group sharing similar concerns.
4) Hybrid: A hybrid cloud includes services using multiple cloud combined together, for example joining services and making some parts private and other parts public or community [14].

The common security issues that need to be addressed for these deployment models are authentication, authorisation, availability, access control and data security. These security issues are so important because each deployment model has a different security level. For example, public cloud is less secure than the other cloud model, so it is more likely to be attacked by malicious hackers to get information that can used then to be hack at the private level. Providers are responsible for service security and they have to stop any unauthorised access or any malicious attacks of the service. Suspicious behaviour includes any malicious attacks and abuse of the service. Consumers take responsibility for information security and data security such as integrity, confidentiality, authorisation and authentication.

There is a list of the top ten obstacles facing cloud computing in [2] summarised in Table II. Armbrust et al. [2] indicate that the consideration for each obstacle will vary from one stakeholder to another (consumer and provider). The first obstacle is Service Availability which has multiple sides. One side is cloud providers offer multiple sites to improve availability, however, consumers may choose to use multiple providers to increase availability. As a result, some parts of the services may become unavailable for some consumers for any time.

There are many reasons that can cause service unavailability such as crashed applications, high loads in the service, and service hijack [15]. Then the consumers will think that the service was down and it is not available to be used. However, services with multiple clouds or multiple sites give more opportunities for an attacker to cause a security threat. An attacker can use a public service to get to unauthorised access to resources or by doing many malicious activities that affect the service. One way to defend this issue is to use quick scale-up method and security monitoring [2]. Scaling method in the cloud is used to control cloud resources, which include two type of scaling, horizontal and vertical [16]. The vertical or scale up is used to increase the virtual resources for restoring and improving performance also known as scaling outward. Service Availability is an issue that can be addressed using this method if any virtual resource becomes unavailable. The horizontal method is to scale upward by running the service in one physical resource. Providing the service from one physical resource or one site is an issue of the service availability.

The second, third and fourth obstacles are about data boundaries between platforms and Data Storage, Data Confidentiality, and Data Transfer. There are many security implications should be considered include loosing data, data leakage, transferring data, and data security. The fifth, sixth, seventh, and eighth obstacles are more technical being related to performance, Scalable Storage, removing errors in a large scale distributing system, and how services can be established with quick scaling getting an overview of service costs. Quick scaling could cause unavailability of the service if there is a very high load tasks which needs to be considered as a security implication of this method. The ninth and tenth obstacles are about service policies and Service Level Agreement (SLA) and Software Licence. The concern here is about the eligibility or the authorisation of using the software and to ensure there is no misuse of the licence [2].

TABLE II. THE TOP TEN OBSTACLES AND CATEGORY [2]

No	Obstacles	Category	Stakeholder Prospective
1	Service Availability	Cloud Service Availability	Consumer
2	Data Storage	Data, Data boundaries	Provider
3	Data Confidentiality	Data, Data boundaries	Consumer
4	Data Transfer	Data, Data boundaries	Consumer
5	Performance unpredictability	Performance, Scalability	Consumer
6	Scalable Storage	Performance, Scalability	Consumer
7	Error of large scale	Performance, Scalability	Provider
8	Quick Scaling	Performance, Scalability	Consumer
9	Service Level Agreement (SLA)	Service policies	Provider, Consumer
10	Software Licence	Service policies	Provider, Consumer

B. Research Method

A Systematic Literature Review (SLR) will identify current research topic related to cloud scheduling and security, then to identify existing gaps, and give an overview of research in the area. To identify gaps papers will be classified into groups depending on their main focus. A recent review [17] shows that most models of cloud security classified to Data as a Service (DaaS), Cloud Storage and research for scheduling just focusing on algorithms. A systematic literature review should contain three stages, which are a plan or a protocol, conducting the review, and reporting the review.

The SLR is needed to identify as much prior research that has been performed in this area and the most relevant to the area of the research topic, which is critical to this research direction and methodology. Also, the outcome of this research is to focus on producing a new model for resource scheduling across cloud security boundaries. Then to obtain a list of the previous research, finding gaps to be extended for further research to find an optimal solution.

C. Research Questions

The research questions will be as the following:

1) What previous research has been done in terms of Scheduling in the Cloud in the presence of security constraints?

2) What constraints other than security need to be considered by each Cloud stakeholder in terms of scheduling in the Cloud?
3) What different types of security constraints have been identified and what do these security constraints defend against?
4) What evaluation metrics have been used to help to evaluate recent research into Scheduling in the Cloud?
5) Based on the research identified, which forms of security aware scheduling merit further research, and why is more research needed and what issues should the further research be addressing?

D. Scope

The following provides the scope for this work using the PICOC model [18].

- **Population:** Published literature papers of scheduling and cloud security.
- **Intervention:** Papers include (Models, surveys, technical report) that address any approaches of scheduling and cloud security.
- **Comparison:** To include comparisons between different scheduling and cloud security models and different approaches.
- **Outcomes of Interest:** The different techniques of scheduling and cloud security models.
- **Context:** To be used by Students and Academic researchers.

III. Search Strategy

This section discusses the choice of the search period, search strings, electronic resources to be used, and the possible use of manual searching.

A. Search Period

The developer of cloud computing came from different area. It started with distributed system and utility computing discussed in the 1990s [19].

Cloud computing as a term will be used for initial search criteria and searching over the period 2006, which is the year of the first cloud conference, to the end of 2015 linking what has been done in the area of Cloud Computing and another related topic such as Cloud Security and Scheduling. Additionally, a manual search will be performed to find an earlier date using Cloud Computing as a term or maybe some other phrases that could be related to the topic such as Grid Computing, Utility Computing, and Distributed System.

B. Search Strings

Basic search strings will be used to try to find papers that relate to the topic and will be filtered in the later stage after applying the including and excluding criteria. Also, basic terms will be used for searching for papers such as (Cloud Security, Cloud Security Model, Cloud Scheduling, Resource Scheduling, Scheduling in the cloud). Then, to find relevant literature reviews using strings as following:

(Cloud Security Model OR Study on Cloud Security, OR Scheduling OR Resource Scheduling) AND (Security in the cloud).

Then:

((((((Cloud) OR (Grid) OR (utilization) AND (Computing))) AND (Security)) AND (Schedul*)) AND (Model*)))

C. Search Engines

To obtain a broad prospective the search will be conducted using the following preferred electronic sources. There are preferred because most papers have been found linked to these search engines and the university library:

- IEEE Xplore – since IEEE are a major publisher of relevant conferences and journals.
- ACM Digital Library – for the same reasons as IEEE.
- To check other search engines for manual search to see what they included such as:
  - web of science
  - ScienceDirect
  - Springer link.

D. Other Search

Other search are conducted are a manual search and a Snowball search.

- A manual search of the first IEEE Cloud Conferences and other cloud conferences will be performed to check the electronic searching and to find out what terms have been used. Also, to extend the search and to find the most relevant papers on the topic that might be overlooked and were not indexed by IEEE or ACM.
- A Snowball search consists of following up the references from the papers obtained through other search forms, in order to identify any other papers that might have been missed by keyword searching. The Snowball search will be performed after making the final selection of papers for inclusion. Particularly, to look at papers that are referenced in sections with such titles as ‘Background’, ‘Related Work’ and ‘Discussion’ since this is where a comparison with similar work is likely to be identified.

IV. Study Selection Criteria and Procedures

This section describes the inclusion/exclusion criteria and the procedures for performing the selection. The scope of this work is confined to those papers that are written in English.

A. Inclusion/Exclusion

The inclusion criteria for selection will be:

- Published Conferences, Workshops, Journals and peer reviewed papers that report on work addressing any aspect of Scheduling in Cloud Security.
- Any previous systematic literature reviews on Scheduling in Cloud Security.
- Where more than one source refers to the same work, the most complete source will be used.
- Where one source refers to more than one piece of work, each relevant work will be counted separately.
- Need to consider the type of research this SLA is interested in - and how the research is conducted - real software implementation, mathematical model or simulation, or thought exercise.

The exclusion criteria will be:

- Sources that are only available as presentations, abstracts, or are otherwise incomplete.
- Forms of publication that have not been subjected to a formal review process, including journals such as ACM Software Engineering Notes (unless containing conference proceedings) and technical reports.
- Opinion paper.

B. Procedures for Selection

After performing the searching phase, the outcomes from the different search engines will be amalgamated into one set of papers. During this process, any obvious duplicates will be removed where a paper has been found by more than one search engine. The inclusion/exclusion criteria will then be applied through the following process.

- Stage 1: Exclusion on the title. This will involve excluding those papers with titles that make it evident that they do not meet the inclusion criteria (e.g. are about some other form of Scheduling or Security).
- Stage 2: Exclusion on abstract. For this, the abstracts were be read and again exclude any papers that are clearly not appropriate.
- Stage 3: Exclusion on full paper. For the remaining candidate papers, obtain the full paper and make a final decision on that basis.
- Stage 4: Resolution of papers and work. This process will identify where the outcomes from a piece of work have been published in more than one paper and where papers are reported.

An initial search has been performed to test the search string on IEEE xplorer, ACM, ScienceDirect, Web of Science, and SpringerLink search engines shown in Fig. 1. In this searching stage the total number of papers from all search engines is 877. Then the search string have been refined to be check that it cover the area and that number of papers found has been increased to 2466.

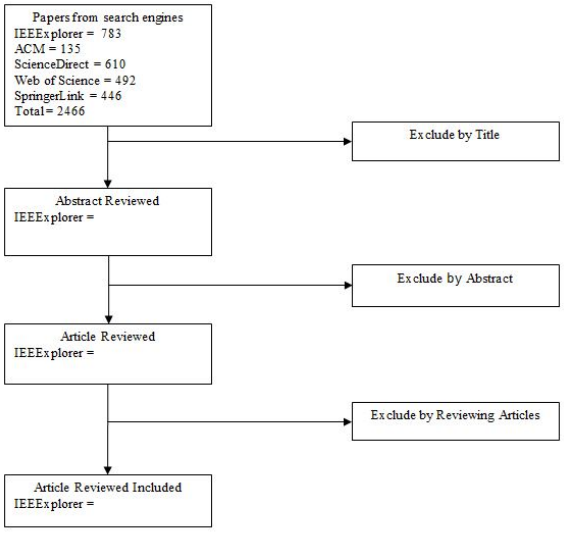

Fig. 1. Procedure for Selection

V. Quality Assessment

The aim of the SLR is to make a decision about the quality of existing work. This depends on the quality score for each paper, and it applies a short quality assessment questionnaires to be completed after performing data extraction. The role of quality assessment is to provide additional information about the primary work that can then be used to assess which ones should be given the greater weighting when drawing any conclusions. This shown as Appendix A.

VI. Data Extraction

For this work, the following proposed questions shown in Table III will be performed for data extraction from each paper:

TABLE III. Questions for Data Extraction

No.	Question	Study Types
1	What was the research question(s)?	
2	What sort of models are used to test the ideas in in the paper(s)?	
3	Which security issues (Table I) are they addressing?	
4	What scheduling and cloud security techniques have been used?	
5	Is definition of the cloud made clear, and if so, what is it?	
6	What cloud implementation(s) have been used?	
7	What was the outcome measure(s)?	
8	What was the reported outcome of the research?	
9	Original work or replication	
10	Appropriate data analysis	
11	Was there a clear link between data and conclusion?	
12	What were the research hypotheses?	
13	Was the context discussed?	
14	Was any comparison discussed?	
15	Were the research questions answered?	
16	What is the approach of the paper including the basic design?	

VII. Synthesis

For this work, any reviews found, systematic or otherwise, will be used to help to check completeness.

A. Synthesis Strategy

This process will include the following three steps:

1) To look at the final set of papers and identify a set of categories from them.
2) Allocating papers to these categories (a paper might fit more than one).
3) To examine the papers in each category to see what could be learned about that topic (this could be a form of vote counting, moderated by quality scores).

B. Threats to Validity

The process of the synthesis could be affected by the threats of validity, and the initial assessment of these as follows:

Internal Validity. Following this protocol allows the selection of accurate papers related to the research topic, and the selections criteria could validate that papers are selected correctly or not.

External Validity. To get more reliable papers that are relevant to the research topic the exclusions criteria will exclude any irrelevant research or any non academic work.

VIII. Limitations

The anticipated outcome of this research may be limited by the following factors:

- The number of work will affect this research, as the previous search did not find that many papers in different areas of the research topic.
- Another limitation is that some work intend to focus on the use of supporting tools and use them just for evaluating their work without discussing the scheduling methodology.
- To consider possible limitation that might arise from the way that this work is conducted (such as missing important papers) and how to mitigate this (such as the use of snowballing, and possibly using a 'gold standard' group of known researches and seeing how many of the searches find).

IX. Discussion

This section discusses the finding of SLR, then it presents the proposed outcome.

This section discusses recent related approaches in the area of cloud security such as Data storage approaches that are related to Data as a Service (DaaS) data storage moving from a single cloud to a multi-cloud, and security models. It also provides some approaches in resource management that used static and dynamic methods focusing on performance.

A review of recent cloud models has been performed to get an overview of the models categories shown in Table IV. Models have been classified to categories related to the main focus of the approaches including Data as a service (DaaS), Infrastructure as a Service (IaaS) and cloud storage. The DaaS models focus on all data security and different from cloud storage which is concerned about data centre security. The IaaS models focus on the infrastructure security.

Table I shows some issues have less attention than others such as Authentication, Accountability, Intrusion, and Reliability. The most focused areas are Integrity, Availability, and Security. Most approaches are related to cloud storage and DaaS which make IaaS need more work especially in security.

The DepSky system [20] addresses the availability and the confidentiality of data in their storage system by using multi-cloud providers, combining Byzantine quorum system protocols, cryptographic secret sharing and erasure codes. Whereas NetDB2-MS [21] is a Model to ensure privacy level in DaaS based on data distributed to different service providers and to employ Shamir's seceret algorithm [22].

The BlueSky System [23] has extended the DepSky system to be more reliable and deal with large storage volume from a cloud provider and to avoid a dedicated hardware server. Similarly, the SafeStore system [24] is more focused on availability not on performance and cost which is quite different than the other systems.

Other approaches like HAIL [26], ICStore [27], SPORC [28], Depot [29], Data storage Models [30], [31] have focused on cloud storage including some data security aspects such as security and data integrity and data confidentiality. They also have similar limitations such as data intrusion and availability.

There are some models at the deployment level which deal with the security risks but with limitations in confidentiality and integrity such as Separation Model - Migration Model - Availability Model - Tunnel Model - Cryptography Model [32].

Data privacy is still a big concern in other Models like Jerico Formu's Cloud Cube Model [17], Hexagon model [17], Multi-Tenancy Cloud Model [33], Cloud Risk Accumulation Model [34], and the Mapping Model [17], [33]. The logging approach [35] ensures that the log files can mitigate the risks to benefit both sides of accountability, security, performance, and scalability.

Other work in scheduling such as [3] takes into consideration tasks priorities then assign them to be executed over the allocated resources. If there more than one task for each resource, it will be scheduled with different methods depending on what is better for each resource. Then it will use parallel running for all tasks. This work assigned dependent tasks first to run first then non dependent one that to minimise the deadlock situation.

Table V shows some approaches that related to resource management used static and dynamic methods and focusing on performance.

Approaches by Li et al. [36] and Yazir et al. [37] relate to resource scheduling using static and dynamic mechanism but they did not include any security factors to avoid any security risks. Static scheduling mechanism such as the approach introduced by Jiayin et al. [38] offers a static scheduling solution to improve service performance over virtual machines. The tasks are executed on certain cloud resources based on the static resource allocation. It aims to regulate many resources utilisation of service level objective of applications SLOs. Also, in [38] propose an algorithm that adjust resource

TABLE IV. REVIEW OF CLOUD MODELS

Ref	Category			Main Focus												
	DaaS	IaaS	Cloud storage	Availability	Confidentiality	Reliability	Intrusion	Integrity	Fault tolerance	Recovery fail	Cost	Scalability	Performance	Accountability	Latency	Security	Authentication
DepSky [20]	√			√	√												
Bluesky [23]	√																
SafeStore [24]	√				√												
NetDB2-MS [21]	√			√			√	√									
NCCloud [25]			√						√	√	√						
HAIL [26]			√	√				√									
ICStore [27]			√				√										
SPORC [28]			√	√													
Depot [29]			√	√						√					√		
Logging Solutions [35]		√										√	√	√			
Venus [31]			√					√									
TCCP [42]		√		√				√									
CCM [17]																√	
Hexagon Model [17]																√	
MTCM [17]																√	
CSA [17]																√	
Mapping model[17]																√	
Separation Model [32]									√								
Migration Model [32]								√								√	
Availability Model [32]				√												√	
Tunnel Model [32]								√								√	
Cryptography Model [32]					√											√	
NDSM [43]	√		√													√	
Cloud Trust Model [44]	√															√	
DSM [45]	√				√											√	
DSSM [30]	√		√													√	√
SC [3]													√				

allocation based on updating the actual task executions which helps to recalculate the finishing time that assigned to the cloud.

Walsh et al. [39] proposed a utility function as a solution by dividing the architecture into two-layers (local and global). The local layer is responsible for calculating resource allocation dynamically. Whereas, the global layer computes the near optimal configuration of allocating resources based on results provided by the local layer, and to fix the load balancing with the server cluster which also helps applications scalability.

Other approaches that use dynamic mechanism such as Yazir et al. [37] and Slegers et al. [40] include a comparison of static and four heuristic dynamic policies. They showed some differences and presented benefits and weaknesses of using each type in terms of using and managing cloud resources. A price model was introduced by Sharma et al. [41] for dynamic resource management and low cost of cloud service but they did not include the security factor and indicate saving cost on physical resources and maintenance cost as limitations of their model.

As a result of this SLR, the proposed model by Sheikh et al. [47] has considered the over all security discussed by

TABLE V. APPROACHES FOR RESOURCE SCHEDULING

Ref	Resource Management	Static	Dynamic	Performance
Adaptive management of virtualised resources [36]	√	√		√
Adaptive resource allocation [38]	√	√		√
Dynamic resource allocation [37]	√		√	√
Resource allocation for multi-tier [46]	√		√	√
Resource Allocation Policies [40]	√		√	√

Watson [48] to develop Scheduling Security Model (SSM) to address the issues found in other approaches by this SLR such as security and cost.

X. CONCLUSION

This paper has briefly introduced an over view of cloud computing including definition, architecture, obstacles facing cloud growth. Then presented the research method and explained why SLR is important to this research. After that, it discussed the search strategy identifying the search period, strings, search engines. Also, it described the inclusion/exclusion criteria, and the procedures of selection. Next, it explained the aim of SLR, then presented how the data will be extracted from each paper and it discussed the synthesis strategy and the threats of validity. After, it addressed limitation and factors that could affect this research. Finally, it presented the current finding of SLR from the reviewed paper and proposed solution. The proposed solution SSM has developed to cover some issues.

ACKNOWLEDGEMENTS

This research protocol has been prepared following the structure provided in [49]. Moreover, thanks to Taif University in Kingdom of Saudi Arabia for the funding.

REFERENCES

[1] K. Yang G, W. Yu, P. ByoungSeob and C. Hyo Hyun, *A heuristic resource scheduling scheme in time-constrained networks*, Computers & Electrical Engineering, Elsevier, 54, 1–15, 2016.

[2] M. Armbrust, A. Fox, , R. Griffith, A. Joseph, R. Katz, A. Konwinsky, L. Andrew, P. Gunho, A. David, A. Rabkin and I. Stoica, *Above the clouds: a Berkeley view of cloud computing*, University of California at Berkeley, 2009.

[3] L. Tripathy and R.R. Patra, *Scheduling in cloud computing*, International Journal on Cloud Computing: Services and Architecture (IJCCSA), 4(5), pp.21-7, 2014.

[4] Wu. Fuhui, Wu. Qingbo and T. Yusong, *Workflow scheduling in cloud: a survey*, The Journal of Supercomputing, Springer, 71, 9, 3373–3418, 2015.

[5] S. Sing and I. Chana, *A survey on resource scheduling in cloud computing: Issues and challenges*, Journal of Grid Computing, Springer, 14, 2, 217–264, 2016.

[6] P. Mell and T. Grance, *The NIST definition of cloud computing*, Computer Security Division, Information Technology, Laboratory, National Institute of Standards and Technology, Gaithersburg, 2011.

[7] P. Patel, A. Ranabahu and A. Sheth, *Service level agreement in cloud computing*, Citeseer, 2009.

[8] F. Panzieri,O. Babaoglu, S. Ferretti, V. Ghini, and M. Marzolla, *Distributed computing in the 21st century: Some aspects of cloud computing*, Springer, 2011.

[9] V. Nallur and R. Bahsoon,*A decentralized self-adaptation mechanism for service-based applications in the cloud*, Transactions on Software Engineering, IEEE, 39, 5, 591–612, 2013.

[10] A. Abdelmaboud, D. Jawawi, I. Ghani, A. Elsafi and B. Kitchenham, ,*Quality of service approaches in cloud computing: A systematic mapping study*, Journal of Systems and Software, Elsevier, 101, 159–179, 2015.

[11] R. Shelke and R. Rajani, *Dynamic resource allocation in cloud computing*, International Journal of Engineering Research and Technology, ESRSA, 2, 10, 2013.

[12] S. Subashini and V. Kavitha, *A survey on security issues in service delivery models of cloud computing*, Journal of network and computer applications, Elsevier, 34, 1, 1–11, 2011.

[13] T. Dillon, C. Wu, and E. Chang, *Cloud computing: issues and challenges*, International Conference on Advanced Information Networking and Applications, IEEE, 27–33, 2010.

[14] D. Goutam, A. Verma, N. Agrawal, *The performance evaluation of proactive fault tolerant scheme over cloud using CloudSim simulator*, International Conference on the Applications of Digital Information and Web Technologies (ICADIWT), IEEE, 171–176, 2014.

[15] S. Ramgovind, M. Eloff, and E. Smith,*The management of security in cloud computing*, Information Security for South Africa, IEEE, 1–7, 2010.

[16] R. Patil and RK. Singh, *Scaling in Cloud Computing*, International Journal of Advance Research, IJOAR, 1, 21–27, ISSN:2320-9194, 2013.

[17] V. Chang,D. Bacigalupo, G. Wills and D. De Roure, *A categorisation of cloud computing business models*, Proceedings of the IEEE/ACM International Conference on Cluster, Cloud and Grid Computing, IEEE Computer Society, 509–512, 2010.

[18] M. Petticrew and H. Roberts, *Systematic reviews in the social sciences: A practical guide*, John Wiley & Sons, 2008.

[19] I. Foster, Y. Zhao, I. Raicu and S. Lu, *Cloud computing and grid computing 360-degree compared*, Grid Computing Environments Workshop, IEEE, 1–10, 2008.

[20] A. Bessani, M. Correia, B. Quaresma, F. André and P. Sousa, *DepSky: dependable and secure storage in a cloud-of-clouds*, ACM Transactions on Storage (TOS), ACM , 9, 4, 12, 2013.

[21] M. Alzain, B. Soh and E. Pardede, *A new model to ensure security in cloud computing services*, Journal of Service Science Research, Springer, 4, 1, 49–70, 2012.

[22] A. Shamir, Adi, *How to share a secret*, Communications of the ACM, ACM, 22, 11, 612–613, 1979.

[23] M. Vrable, S. Savage, GM. Voelker, *BlueSky: a Cloud-Backed File System for the Enterprise*, Proceedings of the 10th USENIX Conference on File and Storage Technologies, USENIX Association, 19–19, 2012.

[24] R. Kotla, L. Alvisi and M. Dahlin, *SafeStore: a durable and practical storage system*, USENIX Annual Technical Conference, 129–142, 2007.

[25] Tu. Hu, HCH. Chen,P. Lee and Y. Tang, *NCCloud: Applying Network Coding for the Storage Repair in a Cloud-of-Clouds*, FAST, 21, 2012.

[26] K. Bowers, A. Juels and A. Oprea, *HAIL: a high-availability and integrity layer for cloud storage*, Proceedings of the 16th ACM conference on Computer and communications security, ACM, 187–198, 2009

[27] C. Cachin, R. Haas and M. Vukolic, *Dependable storage in the intercloud*, IBM research, 3783, 1–6, 2010.

[28] AJ. Feldman, WP. Zeller, MJ. Freedman and EW. Felten, *SPORC: Group Collaboration using Untrusted Cloud Resources*, OSDI, 10, 337–350, 2010.

[29] P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, M. Walfish, *Depot: Cloud storage with minimal trust*, Transactions on Computer Systems (TOCS), ACM, 29, 4, 12, 2011.

[30] HB. Patel, DR. Patel, B. Borisaniya and A. Patel, *Data storage security model for cloud computing*, International Conference on Advances in Communication, Network, and Computing, Springer, 37–45, 2012.

[31] A. Shraer, C. Cachin, A. Cidon, I. Keidar, Y. Michalevsky, and D. Shaket, *Venus: Verification for Untrusted Cloud Storage*, Proceedings of the 2010 ACM workshop on Cloud Computing Security Workshop, ACM, 19–30, 2010,

[32] G. Zhao, C. Rong, MG. Jaatun, FE. Sandnes, *Deployment models: Towards eliminating security concerns from cloud computing*, International Conference on High Performance Computing and Simulation (HPCS), IEEE, 189–195, 2010.

[33] J. Che, Y. Duan, T. Zhang and J. Fan, *Study on the security models and strategies of cloud computing*, Procedia Engineering, Elsevier, 23, 586–593, 2011.

[34] G. Brunette and R. Mogull, *Security guidance for critical areas of focus in cloud computing*, Cloud Security Alliance, 2, 1, 1–76, 2009.

[35] W. Wongthai, F. Rocha, and A. Van Moorsel, *Logging Solutions to Mitigate Risks Associated with Threats in Infrastructure as a Service Cloud*, International Conference on Cloud Computing and Big Data (CloudCom-Asia), IEEE, 163–170, 2013.

[36] Q. Li, Q. Hao, L. Xiao and Z. Li, *Adaptive Management of Virtualized Resources in Cloud Computing using Feedback Control*, First International Conference on Information Science and Engineering, IEEE, 1, 99–102, 2009.

[37] YO. Yazir, C. Matthews, R. Farahbod, S. Neville, A. Guitouni, S. Ganti and Y. Coady, *Dynamic resource allocation in computing clouds using distributed multiple criteria decision analysis*, International Conference on Cloud Computing, IEEE, 3, 91–98, 2010.

[38] J. Li, M. Qiu, JW. Niu, Y. Chen and Z. Ming, *Adaptive Resource Allocation for Preemptable Jobs in Cloud Cystems*, International Conference on Intelligent Systems Design and Applications, IEEE, 10, 31–36, 2010.

[39] WE. Walsh, G. Tesauro, JO. Kephart, and R. Das, *Utility Functions in Autonomic Systems*, Proceedings on International Conference of Autonomic Computing, IEEE ,70–77, 2004.

[40] J. Slegers, I. Mitrani and N. Thomas, *Static and Dynamic Server Allocation in Systems with on/off Sources*, Annals of Operations Research, Springer, 170, 1, 251–263, 2009.

[41] B. Sharma, R. Thulasiram, P. Thulasiraman, S. Garg and R. Buyya, *Pricing Cloud Compute Commodities: a Novel Financial Economic Model*, Proceedings of the 2012 12th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGRID), IEEE, 451–457, 2012.

[42] N. Santos, KP. Gummadi and R. Rodrigues, *Towards Trusted Cloud Computing*, HotCloud, 9, 3–3, 2009.

[43] Sh. Ajoudanian and Mr. Ahmadi, *A novel data security model for cloud computing*, International Journal of Engineering and Technology, IACSIT Press, 4, 3, 326, 2012.

[44] H. Sato, A. Kanai and S. Tanimoto, *A cloud trust model in a security aware cloud*, International Symposium on Applications and the Internet (SAINT), IEEE, 10, 121–124, 2010.

[45] Z. Xin, L. Song-qing and L. Nai-wen, *Research on cloud computing data security model based on multi-dimension*, International Symposium on Information Technology in Medicine and Education (ITME), IEEE, 2, 897–900, 2012.

[46] H. Goudarzi and M. Pedram, *Multi-dimensional SLA-based resource allocation for multi-tier cloud computing systems*, International Conference on Cloud Computing (CLOUD), IEEE, 324–331, 2011.

[47] A. Sheikh, M. Munro and D. Budgen, *Scheduling Security Model (SSM) for a Cloud Environment*, Conference of Cloud Computing, ACM,2,1, pp 1-15, 2018.

[48] P. Watson, *A multi-level security model for partitioning workflows over federated clouds*, Journal of Cloud Computing, Springer,1,1, pp 1-15, 2012.

[49] D. Budgen, *Protocol for a Systematic Literature Review on Empirical Studies of Software Visualisation*, 2011.

APPENDIX

The questionnaire in Table VI will be used to produce a quality score for each paper. Each question should be answered either yes/no (Y/N) or yes/partially/no (Y/P/Y) and there will provision for a short comment where appropriate. Values will be scored as Y=1, P=0.5 and N=0 to provide an overall quality for each paper.

TABLE VI. QUALITY QUESTIONNAIRE

No.	Question	Score	Comment
1.	Does the paper clearly state the aims of the research?	Y/N	
2.	Does the paper answer the research question?	Y/P/N	
3.	Is there any comparison?	Y/N	
4.	Does the paper adequately describe the research Methodology?	Y/P/N	
5.	Was the scheduling technique(s) adequately defined?	Y/P/N	
6.	Does the paper include defined data collection measures	Y/P/N	
7.	Does the paper defined the data collection procedures	Y/P/N	
8.	Are there any potential confounding factors adequately controlled for the analysis?	Y/N	
9.	Does the paper discuss experiment environments?	Y/N	
10.	Does the paper include and discuss of the limitation of the research?	Y/P/N	
11.	Does the paper explain what security issue is addressed / corrected?	Y/P/N	